

# Exhibit N

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA  
ALEXANDRIA DIVISION**

<b>BMG RIGHTS MANAGEMENT</b>	)	
<b>(US) LLC, and ROUND HILL</b>	)	
<b>MUSIC LP</b>	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 1:14-cv-1611(LO/JFA)
	)	
<b>COX COMMUNICATIONS, INC.,</b>	)	
<b>COXCOM, LLC</b>	)	
	)	
Defendants.	)	
	)	

**[REDACTED]**

**MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION *IN LIMINE* NO. 6 TO  
EXCLUDE ARGUMENT THAT COX IS NOT LIABLE FOR INFRINGEMENT OVER  
ITS NETWORK BY USERS OTHER THAN NAMED ACCOUNT HOLDERS**

Plaintiffs BMG Rights Management (US) LLC and Round Hill Music LP respectfully submit this Memorandum in Support of their Motion *in Limine* to preclude Defendants Cox Communications, Inc. and CoxCom, LLC (collectively “Cox”) from arguing that they are not liable because Cox network users other than named Cox account holders are responsible for the infringements at issue.

Plaintiffs, through their agent Rightscorp, have identified rampant infringement of their copyrights by users of the Cox network traceable to Cox-assigned IP addresses. Nonetheless, Cox apparently intends to defend this case by arguing that the actual users committing the infringements may be household members other than the named account holder, such as children, spouses, nannies, etc., or third parties connecting to the internet via Cox subscribers’ unsecured wireless networks.

This is a legally irrelevant distinction that can only confuse the jury and mislead them into ignoring Cox's legal liability for infringement that occurs over its network. Cox is contributorily liable where it knows of and materially contributes to infringement occurring over its network and it is vicariously liable for infringement where it has the right to put a stop from that infringement but benefits by allowing it to continue. *See Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.* 545 U.S. 913, 930 (2005); *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 550 (4th Cir. 2004). This is true whether the infringer is the named account holder or another user of Cox's network, such as a spouse or other household member.

Cox's arguments on this score are doubly misleading because they are speculative and have no foundation in admissible evidence. Cox requires its users to secure their wireless networks and repeatedly warns them of the need to do so. And Cox has no evidence that anyone other than their subscribers is responsible for the illegal downloading of music over the Cox network. Cox should be precluded from offering confusing, baseless, and legally irrelevant arguments about whether its named account holders or other users of their home networks are responsible for infringement over the Cox network and traceable to Cox IP addresses.

## I. Applicable Legal Standard

Only relevant evidence is admissible at trial, Fed. R. Evid. 402, and the Court may exclude otherwise relevant evidence "if its probative value is substantially outweighed by the danger of unfair prejudice." Fed. R. Evid. 403. Evidence may be excluded when there is a significant danger that the jury might base its decision on emotion or where it would distract reasonable jurors from the real issues in a case. *See Tennison v. Circus Circus Enters.*, 244 F.3d 684, 690 (9th Cir. 2001). The purpose of a motion *in limine* is to allow a court to rule on evidentiary issues in advance of trial in order to avoid delay, ensure an expeditious trial, and

focus on the issues the jury will consider. *See United States v. Brawner*, 173 F.3d 966, 970 (6th Cir. 1999). The decision to grant a motion *in limine* is within the Court's discretion. *United States v. White*, 405 F.3d 208, 212 (4th Cir. 2005).

## **II. Cox is Liable for Any Infringement that Occurs Over its Network.**

Cox's open WiFi arguments are irrelevant to and will distract from the key issues in this case: whether the infringement of Plaintiffs' works using Cox's network occurs with Cox's knowledge or constructive knowledge (contributory liability) and whether Cox declines to exercise its ability to stop or limit that infringement while benefitting from the revenue associated with the accounts through which that infringement occurs (vicarious liability). Cox's contributory and vicarious liability for infringement using its network does not depend on whether the named account holder is himself downloading or uploading the infringing material as opposed to another user of the Cox internet connection. Cox is secondarily liable for any such infringement using its network, regardless of whether the account holder or another network user is infringing.

As Plaintiffs explained in their summary judgment opposition, the question in a secondary liability case is whether "users of [the defendant's] services" have engaged in direct infringement, not each infringer's specific identity. *Columbia Pictures Indus. v. Fung*, 710 F.3d 1020, 1034 (9th Cir. 2013) (emphasis added); *In re Aimster Copyright Litig.*, 334 F.3d 643, 646 (7th Cir. 2003) (finding secondary liability where direct infringers could conceal their true identity); *Arista Records, LLC v. Lime Grp., LLC*, 784 F. Supp. 2d 398, 423-24 (S.D.N.Y. 2011) (evidence of downloads from "LimeWire users" established direct infringement); *Sega Enters., Ltd. v. MAPHIA*, 857 F. Supp. 679, 686-87 (N.D. Cal. 1994) (direct infringement where "unknown users" uploaded Sega games). Cox does not get a pass on enabling infringement

because the infringer's internet account happened to be in the name of a different household member. Once Rightscorp data shows infringement by a particular Cox subscriber account at a particular Cox IP address, it does not matter that the infringer happens to be a household member or other network user rather than the named account holder.

Indeed, Cox's own Acceptable Use Policy holds each subscriber responsible for infringement occurring over their account happens on their account – either by a household member or a WiFi poacher. Dkt. No. 317, Theodore Decl., Ex. 10 at 2 (“You are solely responsible for any information that is transmitted from your IP address . . .”); *id.* at 2-3 (requiring subscribers to secure their wireless networks). This is consistent with Congress's intent in enacting the DMCA, in which it considered “subscribers” to include their “household members.” S. Rep. No. 105-190 at 52 n. 24 (1998).

### **III. Cox Has No Evidence that Wifi-Poaching Non-Subscribers Are Responsible for the Infringements**

Cox's suggestions that non-subscribers are responsible for the infringements at issue are also entirely speculative. While conceding that the infringements at issue have been traced to Cox IP addresses, Cox hypothesizes that this is because non-Cox subscribers are accessing Cox subscribers' unsecured wireless networks to share files. But it has no evidence that this is the case.

First, Cox offers no evidence that open WiFi is prevalent among Cox residential users. On the contrary, Cox's subscriber agreement and acceptable use policy require subscribers to password protect their wireless networks. According to Cox, account holders whose IP addresses have been identified in infringement notices are told to secure their wireless network in every warning email, upon self-reactivating from a suspension, and every time they must speak

to a Cox representative. Dkt. No. 397, Zabek Decl. ¶ 9. Cox's repeat infringers have been told over and over to secure their wireless. *Id.*

Indeed, Cox's own abuse staff acknowledge that WiFi poachers are not the issue. See Dkt. No. 389, Allan Decl. Ex. 27 (Abuse manager Zabek: [REDACTED] [REDACTED]). In private they joke about how open WiFi arguments are an unconvincing legal smokescreen by which repeat infringers may deny liability. See Dkt. No. 389, Allan Decl., Ex. 49 (Zabek noting that subscribers [REDACTED] [REDACTED]). Cox should not be allowed to mislead the jury with this baseless distraction.<sup>1</sup>

The only affirmative "evidence" of "stolen WiFi" that Cox has cited is a blog post (<http://www.cnet.com/news/more-people-grabbing-wi-fi-from-their-neighbors/>) describing a study conducted by Wakefield Research and the Wi-Fi Alliance. Cox's expert William Rosenblatt uses this blog post to suggest that, in 2011, 32 percent of respondents admitted that they used other people's open WiFi networks. Roberts Decl., Ex. 1, Rosenblatt Expert Report 6.19.2015 at 11 ¶ 33. But Mr. Rosenblatt has no memory of actually looking at the Wakefield study, just at the blog post. See Roberts Decl., Ex. 2, Rosenblatt Tr at 8.5.15 at 50:11-12 ("I honestly can't remember what I looked at other than the article cited here."). And Cox never produced the Wakefield study itself.

Nor does the blog post indicate that the Wakefield study found widespread poaching of residential wireless networks, much less to share infringing files. According to the blog post, the study asked if respondents ever used **any** open wireless networks. While the actual questions

---

<sup>1</sup> Were Cox actually concerned about unauthorized access to its subscribers' wireless networks, it has the tools to [REDACTED] WiFi. But Cox has chosen not to implement them. See Roberts Decl., Ex. 3, COX\_BMG00155440; Roberts, Decl. Ex. 4, COX\_BMG00217801.

used in the study are a matter for speculation, if the blog post is correct, respondents would answer “yes” if they used open WiFi at Starbucks, an airport, a hotel, or any of the host of locations that make WiFi available to the general public. There is no suggestion that the Wakefield study asked whether respondents accessed their neighbors’ wireless networks or if they download free music or video using other people’s WiFi. Nor is there any indication from the report whether respondents have open WiFi at their own residences. In fact, the blog post notes that the study shows that people tend to guard their WiFi closely: “Forty percent of those surveyed said that sharing their Wi-Fi password requires more trust than sharing their house keys.” In any event, a vague blog post about a report that no one has seen, which on its face does not support Cox’s position, is not admissible evidence.

Cox also relies on a line in [REDACTED]

[REDACTED]  
[REDACTED] *Id.* But the phone script provides no factual basis for that proposition, and Rightscorp’s Chief Executive Officer testified that the statement was not accurate. Roberts Decl., Ex. 5, Sabec 7/7/15 Tr. at 173:3-15. Instead, the script reflects that the most common excuse infringers give for illegal file sharing is that someone else did it through unsecured WiFi.

Cox has provided no evidence that open WiFi is prevalent among Cox residential users or that it is the source of the infringements at issue. Cox should not be able to use speculation on this score as a ground to avoid liability.

#### **IV. Conclusion**

For the foregoing reasons, the Court should prohibit Cox from introducing unreliable and unsubstantiated theories regarding the particular users responsible for infringement over the Cox network and traceable to specific Cox IP addresses.

November 6, 2015

Respectfully submitted,

/s/ Jeremy D. Engle

Jeremy D. Engle (VSB No. 72919)  
jengle@steptoe.com  
Paul Gennari (VSB No. 46890)  
pgennari@steptoe.com  
STEPTOE & JOHNSON, LLP  
1330 Connecticut Ave, NW  
Washington, DC 20036  
Tel.: (202) 429-3000  
Fax: (202) 429-3902

Walter D. Kelley, Jr. (VSB No. 21622)  
HAUSFELD, LLP  
1700 K Street, NW  
Washington, DC 20006  
Tel: (202) 540-7157  
Fax: (202) 540-7201

*Of Counsel*

Michael J. Allan (admitted *pro hac vice*)  
William G. Pecau (admitted *pro hac vice*)  
John M. Caracappa (admitted *pro hac vice*)  
Roger E. Warin (admitted *pro hac vice*)  
Stephanie L. Roberts (admitted *pro hac vice*)  
STEPTOE & JOHNSON, LLP  
1330 Connecticut Avenue, NW  
Washington, DC 20036  
Tel.: (202) 429-3000  
Fax: (202) 429-3902

Michael O. Crain  
Crain Law Group, LLC  
The Bottleworks  
297 Prince Avenue, Suite 24  
Athens, Georgia 30601  
Tel. (706) 548-0970  
Fax: (706) 369-8869

*Counsel for Plaintiff*

**CERTIFICATE OF SERVICE**

I hereby certify that on November 6, 2015, I electronically filed a true and correct copy of the foregoing using the Court's CM/ECF system, which then sent a notification of such filing (NEF) to all counsel of record:

Craig C. Reilly (VSB No. 20942)  
craig.reilly@ccreillylaw.com

William J. Dinkin  
Bill.dinkin@gmail.com

/s/ Jeremy D. Engle  
Jeremy D. Engle (VSB No. 72919)  
jengle@steptoe.com  
STEPTOE & JOHNSON, LLP  
1330 Connecticut Ave, NW  
Washington, DC 20036  
Tel.: (202) 429-3000  
Fax: (202) 429-3902